

# IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strike through~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1-3. (Cancelled)

4. (Previously presented) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ ;

$q$  sets of fixed values, where  $q$  is an integer equal to three or more, wherein equations,  $FM_{i,h} = C_h \text{ XOR } L1_i(L2_{i-1}(D_h))$  for  $i \geq 1$ ,  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , where  $i$  is an integer and  $j$  is an integer,

$q$  sets of fixed values, wherein equations,  $(c_{0,j} \text{ XOR } c_{1,j}) = (0101 \dots 01)_2$  or  $(1010 \dots 10)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) = (0101 \dots 01)_2$  or  $(1010 \dots 10)_2$  are satisfied, a fixed table before masking is defined as  $S[x]$ , and  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  for the  $j$ -th fixed value;

linear transform means  $L1_i(x)$  and linear transform means  $L2_i(x)$ , wherein the linear transform means  $L1_i(x)$ , the nonlinear transform means with the masked fixed table  $S_j[x]$  and the linear transform means  $L2_i(x)$  operate in  $i$ -th one of rounds; and

a first selector for selecting one fixed value of the  $h$ -th set of said  $q$  sets of fixed values of said  $q$  sets of fixed tables in response to the random number  $h$ ,

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value..

5-7. (Cancelled)

8. (Previously presented) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ ;

$q$  sets of fixed values, where  $q$  is an integer equal to three or more, wherein equations,

$FM_{0,h} = C_h \text{ XOR } L1_0$  (FMin),  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , are satisfied, where  $FM_{i,h}$  is the  $i$ -th fixed value of the  $h$ -th set of said  $q$  sets of fixed values, where  $i$  is an integer and  $j$  is an integer,

$q$  sets of fixed values, wherein equations,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$  are satisfied, a fixed table before masking is defined as  $S[x]$ , and  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  for the  $j$ -th fixed value;

linear transform means  $L1_i(x)$  and linear transform means  $L2_i(x)$ , wherein the linear transform means  $L1_i(x)$ , the nonlinear transform means with the masked fixed table  $S_j[x]$  and the linear transform means  $L2_i(x)$  operate in  $i$ -th one of rounds; and

a first selector for selecting one fixed value of the  $h$ -th set of said  $q$  sets of fixed values in response to the random number  $h$ ,

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value

9. (Previously presented) The encryption device according to claim 4, said nonlinear transform means being Subbyte means;

the linear transform means  $L1_i(x)$  comprising means for shifting an input, and the linear transform means  $L2_i(x)$  comprising means for mixedcolumning an input.

10-31. (Cancelled)

32. (Previously presented) The encryption device according to claim 4, characterized in that the linear transform means  $L1_i(x)$  is defined as  $L1_i(x) = x$ .

33. (Previously presented) The encryption device according to claim 4, characterized in that the linear transform means  $L2_i(x)$  is defined as  $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$ .

34. (Previously presented) The encryption device according to claim 4, characterized in that the linear transform means  $L2_i(x)$  is defined as  $\text{Shift}(x)$

35. (Previously presented) The encryption device according to claim 8, characterized in that the linear transform means  $L1_i(x)$  is defined as  $L1_i(x) = x$ .

36. (Previously presented) The encryption device according to claim 8, characterized

in that the linear transform means  $L2_i(x)$  is defined as  $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$ .

37. (Previously presented) The encryption device according to claim 8, characterized in that the linear transform means  $L2_i(x)$  is defined as  $\text{Shift}(x)$

38. (Previously presented) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ ;

$q$  sets of fixed values, where  $q$  is an integer three or more, wherein equations,  $FM_{i,h} = C_h \text{ XOR } L1_i(L2_{i-1}(D_h))$  for  $i \geq 1$ ,  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , are satisfied, where  $i$  is an integer and  $j$  is an integer,

$q$  sets of fixed values, where equations,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (1111 \dots 11)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (1111 \dots 11)_2$ , are satisfied, and a fixed table before masking is defined as  $S[x]$  and an  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{h,j}] \text{ XOR } d_{h,j}$  for the  $j$ -th fixed value;

linear transform means  $L1_i(x)$  and linear transform means  $L2_i(x)$ , wherein the linear transform means  $L1_i(x)$ , the nonlinear transform means with the masked fixed table  $S_j[x]$  and the linear transform means  $L2_i(x)$  operate in  $i$ -th one of rounds; and

a first selector for selecting one fixed value of the  $h$ -th set of said  $q$  sets of fixed values in response to the random number  $h$ ;

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value.

39. (Previously presented) The encryption device according to claim 38, characterized in that the linear transform means  $L1_i(x)$  is defined as  $L1_i(x) = x$ .

40. (Previously presented) The encryption device according to claim 38, characterized in that the linear transform means  $L2_i(x)$  is defined as  $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$ .

41. (Previously presented) The encryption device according to claim 38, characterized in that the linear transform means  $L2_i(x)$  is defined as  $\text{Shift}(x)$ .

42-49. (Cancelled)

50. (Previously presented) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ ;

$q$  sets of masked fixed values and  $q$  sets of fixed tables, where  $q$  is an integer equal to three or more, wherein equations,  $FM_{0,h} = C_h \text{ XOR } L1_0$  (FMin),  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , are satisfied, where  $FM_{i,h}$  is the  $i$ -th fixed value of the  $h$ -th set of said  $q$  sets of fixed values, where  $i$  is an integer and  $j$  is an integer,

$q$  sets of fixed values, wherein equations,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$  are satisfied, a fixed table before masking is defined as  $S[x]$ , and  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  for the  $j$ -th fixed value;

a selector for selecting one of said  $q$  sets of fixed tables in response to the random number  $h$ ,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables; and

a plurality of encrypting rounds, wherein  $i$ -th one of said plurality of encrypting rounds comprises the XOR means, the fixed tables, the selector, linear transform means  $L1_i(x)$  and linear transform means  $L2_i(x)$ , for that round, and wherein the fixed tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means  $L1_i(x)$ , the nonlinear transform means with the masked fixed table  $S_j[x]$  and the linear transform means  $L2_i(x)$  operate in that round.

51. (Previously presented) The encryption device according to claim 50, characterized in that the linear transform means  $L1_i(x)$  is defined as  $L1_i(x) = x$ .

52. (Previously presented) The encryption device according to claim 50, characterized in that the linear transform means  $L2_i(x)$  is defined as  $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$ .

53. (Previously presented) The encryption device according to claim 50, characterized in that the linear transform means  $L2_i(x)$  is defined as  $\text{Shift}(x)$ .

54. (Previously presented) An encryption device comprising XOR means and

nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ ;

$q$  sets of masked fixed values and  $q$  sets of fixed tables, where  $q$  is an integer equal to three or more, wherein equations,  $FM_{i,h} = C_h \text{ XOR } L1_i(L2_{i-1}(D_h))$  for  $i \geq 1$ ,  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , are satisfied, where  $FM_{i,h}$  is the  $i$ -th fixed value of the  $h$ -th set of said  $q$  sets of fixed values, where  $i$  is an integer and  $j$  is an integer,

$q$  sets of fixed values, wherein equations,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$  are satisfied, a fixed table before masking is defined as  $S[x]$ , and  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  for the  $j$ -th fixed value;

a selector for selecting one of said  $q$  sets of fixed tables in response to the random number  $h$ ,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables; and

a plurality of encrypting rounds, wherein  $i$ -th one of said plurality of encrypting rounds comprises the XOR means, the fixed tables, the selector, linear transform means  $L1_i(x)$  and linear transform means  $L2_i(x)$ , for that round, and wherein the fixed tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means  $L1_i(x)$ , the nonlinear transform means with the masked fixed table  $S_j[x]$  and the linear transform means  $L2_i(x)$  operate in that round.

55. (Previously presented) The encryption device according to claim 54, characterized in that the linear transform means  $L1_i(x)$  is defined as  $L1_i(x) = x$ .

56. (Previously presented) The encryption device according to claim 54, characterized in that the linear transform means  $L2_i(x)$  is defined as  $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$ .

57. (Previously presented) The encryption device according to claim 54, characterized in that the linear transform means  $L2_i(x)$  is defined as  $\text{Shift}(x)$ .

58-63. (Cancelled)

64. (Previously presented) An encryption device comprising a random number

generator for generating a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ , and a first plurality of encrypting rounds, wherein

$i$ -th one of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto for that round, where  $i$  is an integer;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

$q$  sets of fixed values, where  $q$  is an integer equal to three or more, wherein equations,  $FM_{0,h} = C_h \text{ XOR } L1_0$  (FMin),  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , are satisfied, where  $FM_{i,h}$  is the  $i$ -th fixed value of the  $h$ -th set of said  $q$  sets of fixed values, where  $j$  is an integer,

$q$  sets of fixed values, wherein equations,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$  are satisfied, a fixed table before masking is defined as  $S[x]$ , and  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  for the  $j$ -th fixed value;

a selector for selecting one of said  $q$  sets of fixed values in response to the random number  $h$ ;

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value;

linear transform means  $L1_i(x)$ ;

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed table;

linear transform means  $L2_i(x)$ , wherein the linear transform means  $L1_i(x)$ , the nonlinear transform means with the masked fixed table  $S_j[x]$  and the linear transform means  $L2_i(x)$  operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

65. (Previously presented) The encryption device according to claim 64, characterized in that the linear transform means  $L1_i(x)$  is defined as  $L1_i(x) = x$ .

66. (Previously presented) The encryption device according to claim 64, characterized in that the linear transform means  $L2_i(x)$  is defined as  $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$ .

67. (Previously presented) The encryption device according to claim 64,

characterized in that the linear transform means  $L2_i(x)$  is defined as  $\text{Shift}(x)$ .

68. (Previously presented) An encryption device comprising a random number generator for generating a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ , and a first plurality of encrypting rounds, wherein

$i$ -th one of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto for that round, where  $i$  is an integer;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

$q$  sets of fixed values, where  $q$  is an integer equal to three or more, wherein equations,  $FM_{i,h} = C_h \text{ XOR } L1_i(L2_{i-1}(D_h))$  for  $i \geq 1$ ,  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , are satisfied, where  $FM_{i,h}$  is the  $i$ -th fixed value of the  $h$ -th set of said  $q$  sets of fixed values, where  $j$  is an integer,

$q$  sets of fixed values, wherein equations,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$  are satisfied, a fixed table before masking is defined as  $S[x]$ , and  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  for the  $j$ -th fixed value;

a selector for selecting one of said  $q$  sets of fixed values in response to the random number  $h$ ;

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value;

linear transform means  $L1_i(x)$ ;

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed table;

linear transform means  $L2_i(x)$ , wherein the linear transform means  $L1_i(x)$ , the nonlinear transform means with the masked fixed table  $S_j[x]$  and the linear transform means  $L2_i(x)$  operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

69. (Previously presented) The encryption device according to claim 68, characterized in that the linear transform means  $L1_i(x)$  is defined as  $L1_i(x) = x$ .

70. (Previously presented) The encryption device according to claim 68,

characterized in that the linear transform means  $L2_i(x)$  is defined as  $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$ .

71. (Previously presented) The encryption device according to claim 68, characterized in that the linear transform means  $L2_i(x)$  is defined as  $\text{Shift}(x)$ .

72. (Currently amended) A program stored on a computer or machine-readable storage medium for use in an encryption device, said program operable to effect the steps of:

selecting one set of  $q$  sets of fixed values, where  $q$  is an integer equal to three or more, in response to a random number  $h$ , where  $h$  is an integer between zero and  $q-1$ ;

XORing an input value with an XOR of a key with said selected fixed value in  $i$ -th one of rounds, wherein equations,  $FM_{0,h} = C_h \text{ XOR } L1_0$  (FMin),  $C_h = c_{h,15}c_{h,14} \dots c_{h,0}$ , and  $D_h = d_{h,15}d_{h,14} \dots d_{h,0}$ , are satisfied, where  $FM_{i,h}$  is the  $i$ -th fixed value of the  $h$ -th set of said  $q$  sets of fixed values, where  $i$  is an integer and  $j$  is an integer;

selecting one set  $S_j[x]$  of  $q$  sets of masked fixed tables in response to the random number  $h$  in that round, wherein equations,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111 \dots 11)_2$  and  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111 \dots 11)_2$  are satisfied, a fixed table before masking is defined as  $S[x]$ , and  $i$ -th masked fixed table is defined as  $S_j[x \text{ XOR } c_{i,j} \text{ XOR } d_{i,j}]$  for the  $j$ -th fixed value;

nonlinearly transforming an input value in accordance with said selected set  $S_j[x]$  of fixed tables in that round; and

linearly transforming an input value and the nonlinearly transformed value in that round.